FAA National Software Conference June 2001
DO-254/EUROCAE ED-80 Overview

RTCA DO-254 / EUROCAE ED-80, Hardware Design Assurance Overview

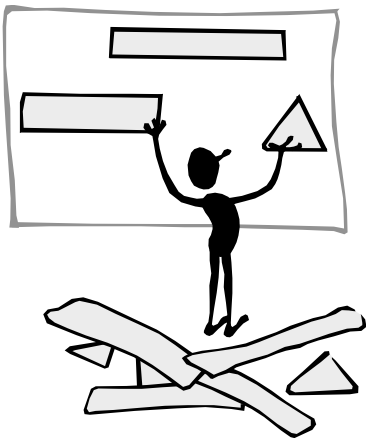
Presented for FAA National Software Conference, June 5, 2001

Will Struck
FAA Transport Airplane Directorate
Standards Staff, ANM-111
will.struck@faa.gov

1

Introduction

- Objective is to present an overview of "new" electronic hardware assurance guidance and discuss current policy and practices associated with the assurance of complex hardware



2

Reasons for Guidance

- Industry "Standard" Guidance Needed
- Hardware, "Firmware" or Software in Disguise (ASIC/PLD's)
- Increasing Complexity & Obsolete Parts
- Testing versus Design Assurance
- Inconsistent Compliance Findings
- Uneven Playing Field

3

Related Regulations and Policy

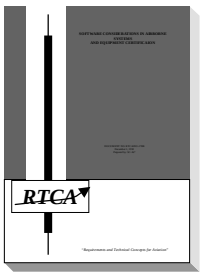
- FAR/JAR 21, 23.1301, 23.1309, 25.1301, 25.1309, etc. and other applicable regulations
- AC/AMJ 23/25.1309-1C/1A, etc.
- FAA TAD PLD Issue Paper
- Changes: 21.91-.101 (TC), 21.115 (STC), 21.611 (TSO)
- FAA Order 8110.4B, Sec. 14, par. c.
- FAA TAD Change Impact Analysis Notice
- DO-178B, Sec. 12.1

4

DO-254/EUROCAE ED-80 Overview

DO-254 / ED-80

- Product of Joint RTCA Special Committee 180 and EUROCAE Working Group 46
- Title: “Design Assurance Guidance for Airborne Electronic Hardware”
- Approved in April 2000 !!



5

DO-254 Outline (1/3)

Foreword
Executive Summary
Membership

- Section 1 Introduction
- 2 System Aspects of Hardware Design Assurance
- 3 Hardware Design Life Cycle
- 4 Planning Process
- 5 Hardware Design Processes

6

DO-254 Outline (2/3)

- Section 6 Validation & Verification Processes
- 7 CM Process
- 8 Process (Quality) Assurance
- 9 Certification Liaison
- 10 Hardware Design Life Cycle Data
- 11 Additional Considerations

7

DO-254 Outline (3/3)

- App A Modulation of Data based on Level
- App B Design Assurance for Levels A & B
- App C Glossary
- App D Acronyms

8

DO-254 Introduction

- 1.1 Purpose - Design Assurance Guidance
- 1.2 Scope - Apply at variety of levels (component, assembly, unit, …)
- 1.4 Related Docs. - ARP's 4754, 4761 DO's -178B, -160D
- 1.5 How to Use Document & 1.8 Document Overview
- Alternative Methods & Processes
- 1.6 Complexity Considerations - Simple versus Complex

9

2 System Aspects

- 2.1-2.1.3 - Info Flow - Systems, Hardware and Software Development Processes
- 2.2 - SSA Process & Assurance Level Definitions
- 2.3 Hardware Safety Assessment - Qualitative, Quantitative, Faults, Errors, Upsets
- 2.3.4 Decision Making Process for Design Assurance Strategy, Pointer to App. B

10

Hardware Design Processes

- 3 HW Life Cycle
- 4 Planning (Objectives, Activities)
- 5.0 ASIC/PLD Map
- 5.1 Requirements Capture (O, A)
- 5.2 Conceptual Design (O, A)
- 5.3 Detailed Design (O, A)
- 5.4 Implementation (O, A)
- 5.5 Production Transition (O, A)
- 5.6 Acceptance Test
- 5.7 Series Production

11

6 Validation and Verification

- 6.1 Validation
  6.1.1 Objective - Validate derived hardware requirements.
  6.1.2 Activities Identify, evaluate, produce evidence, report errors
- 6.2 Verification -
  6.2.1 Objectives
  6.2.2 Activities
- 6.3 V&V Methods
  Testing & Evidence
  Types of Analyses
  Reviews (Requirements, Design)

12

10 Life Cycle Data

- 10.1 Plans (PHAC, HDP, HV&VP, HCMP, HPAP)
- 10.2 Standards (R-D-V&V, Archive)
- 10.3 Design Data (R-CD-DD, Assembly Installation, Interface)
- 10.4 V&V Data
  - Trace, Proc/Results
- 10.5 ATP
- 10.6 PR
- 10.7 CM Records
- 10.8 PA (QA) Records
- 10.9 Accomplishment Summary

13

11 Additional Considerations

- 11.1 Use of Previously Developed HW
- 11.2 COTS Components Usage
  - Electronic Component Mgmt. Prog.
- 11.3 Product Service Experience
  - Acceptability Criteria & Data Assess.
- 11.4 Tool Assessment and Qualification
  - Decision Table, Data

14

Table A-1 Hardware Life Cycle Data by Hardware Design Assurance Level and Configuration Control Code

Data Section	Hardware Life Cycle Data 1	Objectives 2	Submit	Level A	Level B	Level C	Level D
10.1	Hardware Plans						
10.1.1	Plan for Hardware Aspects of Certification	4.1(1,2,3)	S	CC1	CC1	CC1	CC1
10.1.2	Hardware Design Plan	4.1(1,2,3)		CC2	CC2	CC2	NA
10.1.3	Hardware Validation Plan 3 4	4.1(1,2,3); 6.1.1		CC2	CC2	CC2	NA
10.1.4	Hardware Verification Plan	4.1(1,2,3); 6.2.1(1)	S	CC2	CC2	CC2	CC2
10.1.5	Hardware Configuration Management Plan	4.1(4); 7.1(3)		CC1	CC1	CC2	CC2
10.1.6	Hardware Process Assurance Plan	8.1(1,2,3)		CC2	CC2	NA	NA
10.2	Hardware Design Standards						
10.2.1	Requirements Standards 3	4.1(2)		CC2	CC2	NA	NA
10.2.2	Hardware Design Standards 3	4.1(2)		CC2	CC2	NA	NA
10.2.3	Validation and Verification Standards 3	4.1(2)		CC2	CC2	NA	NA
10.2.4	Hardware Archive Standards 3	5.5.1(1); 7.1(1,2)		CC2	CC2	NA	NA
10.3	Hardware Design Data						
10.3.1	Hardware Requirements	5.1.1(1,2); 5.2.1(2); 5.3.1(2); 5.4.1(3); 5.5.1(1,2,3); 6.1.1; 6.2.1(1)		CC1	CC1	CC1	CC1
10.3.2	Hardware Design Representation Data						
10.3.2.1	Conceptual Design Data 3	5.2.1(1)		CC2	CC2	NA	NA
10.3.2.2	Detailed Design Data	5.3.1(1); 5.4.1(2)		5	5	5	5
10.3.2.2.1	Top-Level Drawing	5.3.1(1); 5.4.1(2); 5.5.1(1)	S	CC1	CC1	CC1	CC1
10.3.2.2.2	Assembly Drawings	5.3.1(1); 5.4.1(2); 5.5.1(1)		CC1	CC1	CC1	CC1
10.3.2.2.3	Installation Control Drawings	5.4.1(2); 5.5.1(1)		CC1	CC1	CC1	CC1
10.3.2.2.4	Hardware/Software Interface Data 3	5.3.1(1); 5.5.1(1)		CC1	CC1	CC1	CC1
10.4	Validation And Verification Data						
10.4.1	Hardware Traceability Data	6.1.1(1); 6.2.1(1,2)		CC2	CC2	CC2 6	CC2 6
10.4.2	Hardware Review and Analysis Procedures 3	6.1.1; 6.2.1(1)		CC1	CC1	NA	NA
10.4.3	Hardware Review and Analysis Results 3	6.1.1; 6.2.1(1)		CC2	CC2	CC2	CC2
10.4.4	Hardware Test Procedures 3	6.1.1; 6.2.1(1)		CC1	CC1	CC2	CC2 7
10.4.5	Hardware Test Results 3	6.1.1; 6.2.1(1)		CC2	CC2	CC2	CC2 7
10.5	Hardware Acceptance Test Criteria	5.5.1(3),6.2.1(4)		CC2	CC2	CC2	CC2
10.6	Problem Reports	5.1.1(3); 5.2.1(3); 5.3.1(3); 5.4.1(4); 5.5.1(4); 6.2.1(2)		CC2	CC2	CC2	CC2
10.7	Hardware Configuration Management Records	5.5.1(1); 7.1(1)		CC2	CC2	CC2	CC2
10.8	Hardware Process Assurance Records	7.1(2); 8.1(1,2,3)		CC2	CC2	CC2	NA
10.9	Hardware Accomplishment Summary	8.1(1,2)	S	CC1	CC1	CC1	CC1

Appendix A Notes

1 Data that should be submitted is indicated by an S in the Submit column. CC1 and CC2 data used for certification that need not be submitted should be available. Refer to Section 7.3

2 The objectives listed here are for reference only. Not all objectives may be applicable to all assurance levels.

3 If this data is used for certification, then its availability is shown in the table. This data is not always used for certification and may not be required.

4 This can be accomplished informally through the certification liaison process for Levels C and D. Documentation can be in the form of meeting minutes and and/or presentation material.

5 If the applicant references this data item in required data items, it should be available.

6 Only traceability data from requirements to test is needed.

7 Test coverage of derived or lower hierarchical requirements is not required.

16

Appendix B
Additional Activities for Levels A and B

- Functional Failure Path Analysis (FFPA)
  - Method, Data
- Design Assurance Methods for Levels A and B
  - Arch. Mitigation
  - Service Experience
  - Adv. Verif. Methods

Advanced Verification Methods

- Elemental Analysis (bottom-up)
- Safety Specific (top-down)
- Formal Methods (error detection & preclusion)

17

Recognition by Authorities

- Questions about application:
  ? Apply to just PLD/ASIC or other CEH?
  ? Apply to all FAR parts (23, 25, 27 …)?
  ? Apply to Levels A and B only?
- AC/AMJ in Work?
- TAD “generic” PLD Issue Paper has been updated to recognize DO-254 as a MOC.

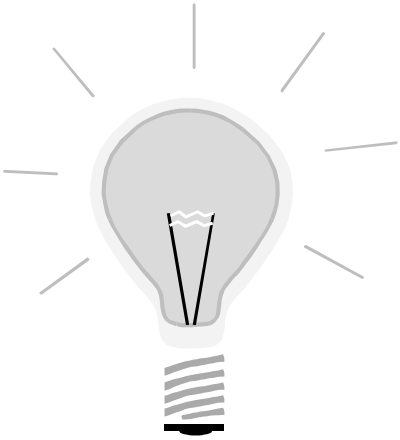
18

Other Resources

- FAA Complex Electronic Hardware Interactive Video Training (IVT) - Video and Workbook
- FAA-Contracted UTRC COTS Hardware Report
- DOT/FAA/AR-95/31, "Design, Test, and Certification Issues for Complex Integrated Circuits"
- Company Hardware Design Assurance Standards and Policy

19

Insights (1/2)



- Section 1.6 - Simple vs Complex
- Section 2.3.1 - Hardware Safety Assessment (HSA) and Hardware Design Assurance Levels

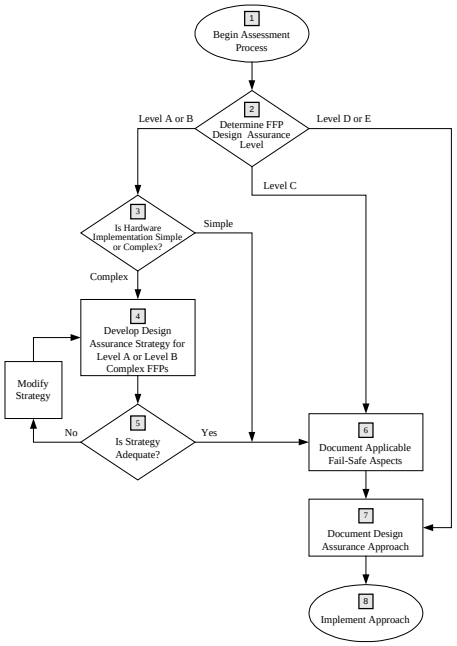
20

Insights (2/2)

- Section 2.3.4 - Decision-Making Process for Assurance Strategy - Pointer to App B
- Appendix B Design Assurance for Levels A & B Functions

21

Figure 2-3
Decision Making Process for Selecting the Hardware Design Assurance Strategy



Summary

- DO-254 somewhat similar to DO-178B
- Has some significant differences:
  - Some differing objectives
  - Data Set
  - Modulation of Data
  - App. B Methods

23